التدابير الوقائية المسبقة
الواجب اتخاذها لمواجهة مخاطر الدفع الالكتروني
Priori precautionary measures to be taken to face the risk of electronic payment

الدكتورة ركاي غنيمة
كلية الحقوق والعلوم اللسياسية
جامعة البليدة 02. الجزائر

الدكتورة زلاسي بشرى
كلية الحقوق والعلوم السياسية
جامعة البليدة 02. الجزائر

تاريخ استلام المقال : 2022-03-25 تاريخ القبول : 2022-04-23 المؤلف المراسل : ركاي غنيمة

ملخص

بذلت الجزائر جهودا كبيرة لتحديث أنظمتها المعلوماتية والدفع وكذا عصرنة المعاملات المالية والمصرفية وسبل معالجة المعلومات بتكريسها مختلف وسائل الدفع الإلكتروني، إلاّ أن هنالك مخاطر مرتبطة باستخدام هذه الوسائل مما يتعين وضع التدابير الوقائية المسبقة للتفادي من المخاطر الناجمة عن استعمال الوسائل الدفع الإلكتروني والتي نص عليها المشرع صراحة كإلزامية التوقيع والتصديق الإلكترونين وكذا حماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية، والتشفير.

تكمن أهمية الموضوع أنه قد يحدث العبث بالأجهزة الالكترونية من قبل الغير ويلحق أضرارا بالأشخاص لذا يجب البحث عن التدابير الوقائية المناسبة لمنع ذلك،والإشكاليةتتمثل: مدى فعالية التدابير الوقائية الأمنية المكرسة قانونا لمواجهة المخاطر الدفع الالكتروني؟

المكالمات المفتاحية: المعالجة – المعطيات الشخصية-التشفير-التصديق-الالكتروني.

ABSTRACT

Algeria his made great ,efforts to modernize itsinformation and payment systems, as well as modernize financial and banking transacttions and information processing methods by dedicating them to various electronic payment methods, however, there are risks associated with the use of these means, which necessitates putting in place appropriate preventive measures to avoid the risks arising from the use of electronic payment methods which are

expressly stipulated by the legislator as mandatory electronic signature and certification, as well as the protection of natural persons in the field of personal data processing and encryption.the importance of the topic is that tampering with electronic devices may occur by others and cause harm to people,so preventive measures must be sought to prevent this,and the problem is,how effective is the security preventive measure legally devoted to confronting the dangers of electronic tampering.

Key WORDS :processing- personal data-encryption-ratification-electronic.

المقدمة

يشهد العالم المعاصر تغيرات جذرية على صعيد أنظمة ووسائل وقنوات الدفع الإلكترونية، والتي لا يمكن للقطاع المصرفي تجاهلها، لاسيما مخاطر أمنية التي عرفت بدورها تطور موازيا، الأمر الذي يلقي على عاتق الجهات الإشرافية والرقابية ذات الصلة في الدولة اتخاذ التدابير الوقائية التي تقلل أو تمنع مثل هذه التجاوزات ذات الطابع الأمني وتعمل على إحباط الهجمات على مكونات النظام قبل تنفيذ عملية احتمالية عليه، وتعزيز بذلك سلامة ومنعة النظام المالي والاقتصادي ككل من أية ممارسات غير مشروعة قد يتعرض لها.

والجزائر على غرار دول العالم تبنت رقمنة الاقتصاد بما فيها تبني استعمال الدفع الإلكتروني، ورغم تأخرها في استخدام هذا النوع من الدفع إلا أنها تحاول جاهدة وضع أنظمة الحماية القانونية الكافية للمعاملات الإلكترونية[1]، ذلك أن العالم الافتراضي يعرضنا لعدد من المخاطر مثل سرقة الهوية، واعتراض أخرين على وسائل الغير واستنكار عملية البيع أو دفع أو تبادل، لذا فإن وضع تدابير أمنية وقائية كتصديق الإلكتروني وحفظ المعطيات ذات الطابع الشخصي بات من إحدى الضروريات.

وتكمن أهمية الموضوع: إن لجوء البعض إلى العبث بالأجهزة الإلكترونية لتخريب وتحريف وسرقة معطيات ذات الطابع الشخصي أثناء معالجتها إلكترونيا أو حفظها، لذا أضحى من الضروري وضع تدابير أمنية وقائية لتصدي لمثل هذه الهجمات الإلكترونية.

والإشكالية المطروحة تتمثل في مدى فعالية ونجاعة التدابير الوقائية الأمنية المسبقة لاسيما تلك التي كرسها المشرع الجزائري في التصدي لمخاطر الدفع الإلكتروني؟ أم أن الأمر يتطلب البحث عن تدابير أخرى أكثر صرامة التي تحول دون حدوث هذه المخاطر؟

للإجابة على هذه الإشكالية قسمت الموضوع إلى ثلاثة محاور:

خصصت المحور الأول: لإجراءات الخاصة بمعالجة المعطيات ذات الطابع الشخصي، والمحور الثاني حول التصديق الإلكتروني أما المحور الثالث تناولت حول التشفير.

1. الإجراءات الخاصة بمعالجة المعطيات ذات الطابع الشخصي

يشكل أمن المعلومات في العصر الحديث حجر الزاوية في عمليات نهضة تكنولوجية المعلومات والاتصالات، حيث أن المساهمة المتاحة للخصوصية تتناسب عكسيا مع التقدم التكنولوجي المعلوماتية والاتصالات[2]، إذ يعمل الحاسوب على جمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد وكل أمر من هذه الأمور تشكل خطرا بشكل أو بآخر على حياة الإنسان الخاصة ويهددها، لهذا فإن الفرد يصبح أسيرا للمعلومات التي جمعتها هذه الآلة عنه، كون أن الشبكات المفتوحة لا تقد=م أي أمان جوهري لاسيما في التجارة الإلكترونية[3]. ومن ثم كان لزاما البحث عن المقصود بالمعطيات ذات الطابع الشخصي ومعالجتها (أولا) وكيفية خضوع المعطيات ذات الطابع الشخصي للمعالجة (ثانيا) وقيود تخزين المعلومات ذات الطابع الشخصي (ثالثا) وأمن وسرية المعطيات أثناء الدفع الإلكتروني (رابعا).

1.1. المقصود بالمعطيات ذات الطابع الشخصي ومعالجتها:

يتعين معرفة ما المقضصود بالمعطيات ذات الطابع الشخصي (**1**)والمعالجة (**2**).

1- تعريف المعطيات ذات الطابع الشخصي:

لم تعد البيانات الشخصية منحصرة في البيانات التقليدية كالاسم واللقب والعنوان البريدي، بل اتسعت هذه البيانات وتنوعت لتشمل صورة الشخص وصوته، كما أنها تشمل بعض البيانات المتعلقة بالشخص ذات من حيث قدرته المالية وتلك المتعلقة بجسم الإنسان "البيانات البيومترية"، لذا يجب البحث عن تعريف الفقهي للمعطيات (أ) ثم التعريف الذي جاء به المشرع الجزائري (ب).

أ- التعريف الفقهي للمعطيات ذات الطابع الشخصي: ذهب الفقه إلى ضرورة احترام سرية البيانات الخاصة بالعملاء بوصفهم المستهلكين، وكذلك احترام حقهم في الخصوصية، يقتضي ذلك الالتزام بعدم نشر أو بث أي بيانات تتعلق بشخصياتهم أو حياتهم الخاصة وكذلك البيانات المصرفية الخاصة بهم[4]، أو إساءة استخدامها وتوجهيهم توجيها منحرف أو مراقبتهم دون علمهم، لأن خصوصية الأفراد وأسرارهم في عالم الإنترنت معرضة للاعتداءات والتحايل وقد تزداد هذه الاعتداءات كما ازدادت استعلامات الدفع الإلكتروني[5].

ويرى الفقهاء أيضا أن حماية خصوصية التعاملات المالية في بيئة الإنترنت أحد أهم ضمانات وجود النشاط التجاري فيها وتطوره، وكما قيل فإن نظام الدفع المالي على الإنترنت بدون نظام حماية للخصوصية سينقلنا من عالم الدفع النقدي المستتر إلى عالم مليء بوسائل الكشف والتعريف، تتزايد فيه قدرة تتبع الأشخاص ومشترياتهم[6].

المعطيات هي معلومات تم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، والمعطيات غير مادية لأنها عبارة عن نبضات الكترونية داخل الحاسب لا يمكن لمسها[7].

ب- التعريف التشريعي لمعطيات ذات الطابع الشخصي: عرف المشرع الجزائري في ضوء القانون رقم 18-07 المؤرخ في 10 يونيو 2018[8] بأنه كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أناده "الشخص المعني" بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته المدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية، أو الثقافية أو الاجتماعية، والأمر يتعلق إذن بجميع أنواع المعلومات المتعلقة بشخص طبيعي التي تمكن من التعريف به على نحو مباشر أو غير مباشر بما في ذلك عن طريق مقاربة المعلومات المتعددة المصادر أو التقاطع فيما بينها.

ويتضح مما تقدم أن البيانات أو المعطيات تعتبر شخصية طالما أنها تتعلق بالأشخاص الطبيعيين الذين تم تحديد هويتهم بشكل مباشر أو غير مباشر، كما أنه يمكن التعرف على شخص وتحديد هويته عندما يظهر اسمه على سبيل المثال في ملف الذي يحتوي على معلومات تسمح بشكل مباشر بتحديد هويته، الاسم ورقم التسجيل أو رقم الهاتف أو الصورة الفتوغرافية أو البيانات البيومترية مثلا بصمة الأصبع أو الحمض النووي، وكذلك جميع المعلومات التي يكون من شأنها تمييز الأشخاص عن غيرهم مثل مكان الإقامة أو المهنة والنوع والسن[9].

2- المقصود بالمعالجة:

أطلق عليها تسمية المعلومات وهي الصورة المحمولة لبيانات المنظمة والمعالجة بطريقة تسمح باستخلاص نتائج نهائية[10].

لا يريد الأفراد أن تكون البيانات الخاصة بهم متوفرة تلقائيا لغيرهم من الأشخاص والمنظمات حتى في حالة أن تكون البيانات مملوكة من طرف آخر، فلهم القدرة على ممارسة

قدر كبير من السيطرة أو التحكم بتلك البيانات وطريقة استخدامها[11]، وهذا الحق مكرس دستوريا في المادة 47:« لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت...».

ويعرف المشرع المعالجة في المادة 03 من القانون رقم 18-07 السالف الذكر بأنها:« كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الايصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الاتلاف».

2.1. كيفية اخضاع المعطيات ذات الطابع الشخصي للمعالجة

يجب أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم ما عدا في حالة موافقتهم الصريحة يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك جمعت من أجلها[12].

إذ لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني ويمكن لهذا الأخير أن يتراجع عن موافقته في أي وقت[13].

تخضع في البداية كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها طبقا للأحكام المنصوص عليها في هذا القانون[14] ويودع التصريح المسبق الذي يتضمن الالتزام بإجراء المعالجة وفقا لأحكام القانون رقم 18-07 لدى السلطة الوطنية ويمكن تقديمه بالطريق الإلكتروني، يسلم وصل الإيداع أو يرسل بالطريق الإلكتروني فورا أو في أجل أقصاه 48 ساعة[15]، ويجب أن يتضمن التصريح ما يأتي: وصف عام يمكن من تقسيم أولي لمدى ملائمة التدابير المتخذة من أجل ضمان سرية وأمن المعالجة[16].

يجب على المسؤول عن المعالجة وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو

التلف أو النشر أو الولوج غير المرخصين، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معينة، وكذا حمايتها من أي شكل من أشكال المعالجة غير المشرعة، ويجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تشملها المعالجة وطبيعة المعطيات الواجب حمايتها ، وحرصا من المشرع فقد أخضع معالجة المعطيات لأمن السيبراني[17]، وكما جاء في محتوى المادة 160 من القانون رقم 18-07 المؤرخ في 10 مايو 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية بأنه:« يلتزم المتعاملون وكذا مستخدموهم باحترام سرية المراسلات الصادرة عن طريق الاتصالات الإلكترونية وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين...».

زيادة على ما تقدم يخضع إنشاء واستغلال شبكات الاتصالات الإلكترونية المفتوحة للجهور وتقديم خدمات الاتصالات الإلكترونية للجمهور إلى احترام مايلي:« شروط خصوصية البيانات والمعلومات التي تم إيصالها بواسطة شبكات الاتصالات الإلكترونية- شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي...».

وفي حالة ما إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطة الوطنية أو الشخص المعني إذا أدى ذلك إلى المساس بحياته الخاصة، ما لم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من قبل مقدم الخدمات، ويجب على كل مقدم خدمات أن يسمك جردا محينا حول الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والإجراءات التي اتخذها بشأنها.

3.1. قيود قانونية الخاصة بحفظ المعطيات ذات الطابع الشخصي

فيما عدا المعطيات الخاصة التي يحظر تخزينها وحفظها، فإن المعطيات الخاصة الأخرى يجوز حفظها ولكن حسب الضوابط والقيود التالية:

1- مشروعية الحصول عل هذه المعطيات بطريقة تخلو من الاحتيال والغش، فلا تحفظ أو تخزن معطيات تتعلق بالحياة الخاصة إلا بعد موافقة صاحب الشأن[18] ذلك ما نصت عليه المادة 07 من القانون رقم 18-07 السالف الذكر.

استثناء من هذا المبدأ، تكون موافقة الشخص المعني واجبة إذا كانت المعالجة ضرورية: لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة – لحماية حياة الشخص المعني.

– لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه، – للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه، ولتنفيذ مهمة تدخل ضمن الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم اطلاعه على المعطيات.

– لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/ أو حقوقه وحرياته الأساسية.

2- يجب أن تكون المعطيات الشخصية مجمعة لغايات محددة وواضحة ومشروعة وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات.

3- ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها.

4- يجب أن تكون المعطيات الشخصية صحيحة وكاملة ومحينة إذا اقتضى الأمر.

5- أن تكون محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها[19].

4.1. أمن وسرية المعطيات الشخصية أثناء الدفع الإلكتروني

أضحت الشبكة المعلوماتية أداة أساسية للتعاملات المالية التي تجري بين الزبون والمؤسسات المصرفية والمورد الإلكتروني، لذلك فإن سرية وأمن المعطيات التي يتم تبادلها عند إبرام صفقات التجارة الإلكترونية خصوصا عندما يتعلق الأمر بأسرار الزبون أو بمسائل مالية كأرقام حسابات المتعاملين و أرقام بطاقات الائتمان تعد ضرورية لنجاح التجارة الالكترونية، بحيث يسمح للمورد الالكتروني وفقا قانون 18-05 المتعلق بالتجارة الالكترونية جمع المعطيات الشخصية المتعلقة بالزبائن وتخزينها كما جاء في محتوى المادة 36 منه التي تنص غلى أنه "ينبغي للمورد الالكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن والزبائن المحتملين ،ألا يجمع إلاّ البيانات الضرورية لإبرام

المعاملات التجارية كما يجب عليه : - الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات ، - ضمان أمن نظام المعلومات وسرية البيانات والتزامه بالأحكام القانونية والتنظيمية المعمول بها في هذا المجال.... كما تخضع منصات الدفع الالكتروني لرقابة بنك الجزائر لضمان استجابتها لمتطلبات التشغيل البيني وسرية البيانات وسلامتها وأمن تبادلها.

2. دور التصديق الإلكتروني في تأمين المعاملات الإلكترونية

للوصول إلى الدور الذي تؤديه جهات التصديق لتأمين المعاملات الإلكترونية يجب معرفة ما المقصود بالتصديق الإلكتروني (أولا) شهادة التصديق الإلكتروني (ثانيا) ثم الالتزامات الاتي تقع على عاتق مؤدى خدمة التصديق الإلكتروني (ثالثا).

1.2. تعريف التصديق الإلكتروني

عرف جانب من الفقه بأنه وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر من خلال التحقق من نسبته إلى شخص محدد وذلك عن طريق جهة محايدة تسمى بمقدم خدمات التصديق أو التوثيق الإلكتروني[20].

أما المؤدي خدمات التصديق الإلكتروني هناك من عرفه بأن: أي شخص طبيعي أو معنوي يستخرج شهادات إلكترونية ويقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية ويضمن تحديد هوية الأطراف المتعاقدة والاحتفاظ بهذه البيانات لمدة معينة ويلتزم باحترام القواعد المنظمة لعمله والتي يتم تحديدها بمعرفة السلطة المختصة[21].

كما تعرض المشرع لتعريف مؤدي خدمات التصديق الإلكتروني في المادة 03 من المرسوم التنفيذي رقم 07-162[22] بأنه:« كل شخص في مفهوم المادة 08-08 من القانون رقم 2000-03 المؤرخ في 05 أوت 2000 والمذكور أعلاه ، يسلم شهادات أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني» وعرفه كذلك في الفقرة 12 من المادة 02 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين بأنه:« شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني».

يتضح جليا من محتوى النصوص القانونية أن مؤدى خدمة التصديق الإلكتروني يعد هيئة عامة أو خاصة تعمل تحت إشراف السلطة التنفيذية، وتتكون غالبا من ثلاثة مستويات مختلفة من السلطة تأتي في المرتبة العليا (السلطة الرئيسية) وهي تختص بالتصديق على تكنولوجيا وممارسات جميع الأطراف المرخص لهم بإصدار أزواج مفاتيح التشفير أو

شهادات تتعلق باستخدام تلك المفاتيح وتليها في المرتبة (سلطة التصديق) وهي جهة خاصة بعملية التصديق على أن المفتاح العام لأحد المستخدمين يناظر بالفعل المفتاح الخاص لذلك المستخدم وفي مستوى أدنى تأتي (سلطة تسجيل محلية) ومهمتها تلقي الطلبات من الأشخاص الراغبين في الحصول على أزواج مفاتيح التشفير- العام والخاص- والتأكد من هوية وشخصية هؤلاء المستخدمين ومنح شهادات تصديق تفيد صحة توقيع العملاء.

ومما تجدر الإشارة إليه أن مؤدى خدمة التصديق يعد شخص ثالث ومستقل عن الأطراف، وحده يتبع تقوية فاعلية نظام التوقيع الإلكتروني لهذا فرض المشرع على عاتق مؤدي خدمة المصادقة أو الشخص الثالث التزامات يتعين عليها مراعاتها عند إصدار الشهادات الإلكترونية، بان تقوم بالتحري حول سلامة المعلومات التي تجمعها من حيث مضمونها ومحتواها وصحة صدورها ممن تنسب إليه، وتصدر بذلك شهادة تصديق إلكترونية تشهد فيها بذلك، ويتم الاعتماد عليها في إتمام المعاملات الإلكترونية.

وتعد الوظيفة الأساسية لجهة التصديق الإلكتروني هو تحديد هوية المتعاملين في التعاملات الإلكترونية وتحديد أهليتهم القانونية في التعامل والتحقق من مضمون هذا التعامل وسلامته وكذلك جديته وبعده عن الغش والاحتيال[23]، وعملها كذلك عل توثيق التوقيع الإلكتروني ومنحه الحجية القانونية في الإثبات من خلال تبيان مدى استجابته للاشتراطات القانونية وضمان عدم إنكار أي من طرفي العقد الإلكتروني لتوقيعه عليه[24].

كما جاء في محتوى المادة 03 من المرسوم التنفيذي رقم 07-162 السالف الذكر أن الشهادة الإلكترونية: «وثيقة في شكل إلكتروني تثبت الصلة بين معطيات التوقيع الإلكتروني والموقع...»، واعتبر المشرع شهادة التصديق بأنها إلكترونية المصدر ووظيفتها تتمثل في الربط بين معطيات التوقيع الإلكتروني والموقع.

زيادة على ما تقدم فإن الدفع في المعاملات الالكترونية يجب أن يكون وصل موقع الانترنت الخاص بالمورد الالكتروني بمنصة الدفع الالكترونية مؤمنا بواسطة تصديق الكتروني[25].

2.2. الالتزامات التي تقع على عاتق مؤدي خدمة التصديق الالكتروني

لا بد أن يتقيد بالالتزامات التي تهدف إلى حماية المعطيات والبيانات الشخصية، وتلك التي تتعلق بصحة المعلومات موضوع شهادة المصادقة.

1- الالتزامات التي تهدف إلى حماية البيانات الشخصية:

والتي تتمثل فيمايلي:

أ- ضرورة الحصول على ترخيص من الجهة المختصة قبل بدء ممارسة خدمة التصديق الالكتروني: طبقا لما جاء في المادة 33 من القانون رقم 15-04 فإن نشاط تأدية خدمات التصديق الإلكتروني يخضع إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني، وتمنح شهادة التأهيل قبل الحصول على الترخيص لمدة سنة واحدة قابلة للتجديد مرة واحدة، تخوّل هذه الشهادة لحاملها بتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني.

ب- الحفاظ على سرية البيانات: ويقصد بالسرية الحفاظ على البيانات ذات الطابع الشخصي المقدمة من العميل إلى الجهة المختصة بإصدار شهادة التوثيق الإلكتروني ومن خلال محتوى المادتين 42 و43 من القانون رقم 15-04 ألزم المشرع مؤدى خدمة التصديق الإلكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة، ويتعين عليه الاكتفاء بالبيانات الضرورية لإنشاء الشهادة دون أي بيانات أخرى[26] ولا يمكنه استعمال هذه البياناتت إلا في إطار وظيفته كمؤدى لخدمة التصديق الإلكتروني ، ولا يمكنه بأي شكل من الأشكال إدارة المعطيات المجمعة واستثمارها في أغراض أخرى إلا بعد الحصول على موافقة الشخص المعني أو تبعا للحالات التي يجيزها القانون، كما ألزم المشرع حسب المادة 47 من نفس القانون مؤدى خدمات التصديق الإلكتروني بتحويل المعلومات المتعلقة بشهادة التصديق بعد انتهاء صلاحيتها إلى السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها.

2- الالتزامات الخاصة بصحة البيانات والمعطيات موضوع شهادة المصادقة:

تتمثل هذه الالتزامات فيمايلي:

أ- التحقق من صحة المعطيات: تستوجب المادة 14 من القانون رقم 15-04 على مؤدى خدمة التصديق الإلكتروني، وقبل منح شهادة التصديق أن يتحقق من مطابقة الآلية المؤمنة لإنشاء البيانات المعروضة عند التحقق من التوقيع الالكتروني، هذا وحسب المادة 53 من نفس القانون يكون مؤدى خدمة التصديق الإلكتروني الذي سلم الشهادة مسؤولا عن الضرر الذي يلحق بأية هيئة أو شخص طبيعي أو معنوي اعتمد على هذه الشهادة، وذلك فيما يخص:

- صحة جميع المعطيات والبيانات الواردة في شهادة التصديق الإلكتروني في التاريخ الذي منحت فيه وعن وجود جميع البيانات الواجب توافرها فيها.

- التأكد عند منح الشهادة أن الموقع الذي تم تحديد هويته في الشهادة يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقيق من التوقيع المقدمة.
- التأكد من إمكانية استعمال بيانات إنشاء التوقيع والتحقق منه بصفة متكاملة[27].

ب- ضمان آلية تأمين وحماية البيانات لإنشاء التوقيع الالكتروني: طبقا لمحتوى المادة 11 من القانون رقم 15-04 السالف الذكر: يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل مايلي: «ألا يمكن عمليا مصادقة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة وأن تتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد».

- ألاّ يمكن ايجاد البيانات المستعملة لإنشاء التوقيع الالكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.
- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.
- يجب أن لا تعدل البيانات محل التوقيع وأن تمنع عرض هذه البينات على الموقع قبل عملية التوقيع.

3- التزام بإلغاء شهادة التصديق الإلكتروني:

ويكون حسب الحالات الواردة في المادة 45 من القانون 15-04 المذكورة أعلاه وأبرزها:

حالة طلب الإلغاء صاحب الشهادة الذي سبق تحديد هويته، وقد تكون المعطيات الواردة في شهادة التصديق الالكتروني عير مطابقة للواقع، أو نم انتهاك سرية بيانات إنشاء التوقيع.

حالة وفاة الشخص الطبيعي أو حل الشخص المعنوي صاحب الشهادة، وكذلك حالة إنتهاء مدة صلاحية الشهادة، أو أن هذه الأخيرة أصبحت غير مطابقة لسياسة التصديق أو رغبة مقدم خدمات التصديق الالكتروني في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الالكتروني أو بأي فعل قد يؤدي إلى ذلك، وعند صدور حكم قضائي بإلغاء شهادة التصديق.

4. التشفير الإلكتروني لمعطيات كوسيلة لتأمين الدفع الإلكتروني:

يعمل التشفير على تأمين المعاملات الإلكترونية بصفة عامة التي يمكن أن تطال الأجهزة والنظم الإلكترونية المستخدمة في مجال النقود والتجارة الإلكترونية بالنظر لما يحققه التشفير من سرية وخصوصية المراسلات والبيانات والاتصالات المستخدمة في الصفقات، إضافة إلى الاستعمالات المختلفة للتشفير في نظام التجارة الإلكترونية والتي تهدف إلى توفير الثقة في المعاملات المصرفية والتجارة الإلكترونية[28].

سأتطرق إلى تعريف التشفير وأهميته (أولا) ثم ضوابط التشفير (ثانيا) أنظمة التشفير (ثالثا).

1.3. تعريف التشفير وأهميته

تعريف التشفير (1) وأهميته في دفع المخاطر (2).

1- تعريف التشفير:

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة أو تحويلها إلى رموز غير ذات معنى، حيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الاستفادة منها، لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة إلى نصوص مشفرة وغير مفهومة، وتبنى على أساس أن كل معلومة تحتاج لفكها وإعادتها إلى الوضع الأصلي[29].

ويعرف كذلك تحويل المعلومات إلى شفرات غير مفهومة لمنع الأشخاص غير المرخص لهم من الاطلاع عليها، أو مزج المعلومات الحقيقية بمعلومات وهمية، ينتج عنها توليد معلومات جديدة لا يمكن معرفة المعلومات الحقيقية فيها، دون معرفة طريقة التشفير المتبعة والمفتاح السري المستخدم في ذلك[30]، كتشفير أرقام بطاقات أو غيرها من البيانات وعملية التشفير تعمل على تحويل النصوص العادية إلى نصوص مشفرة وذلك باستخدام مفاتيح، وهذه الأخيرة تستند إلى صيغ رياضية معقدة (خوارزميات) وتعمد قوة وفعالية التشفير على أساسين: الخوارزمية وطول المفتاح (مقدرا بالبت Bits) أما فك التشفير هو عمله إعادة تحويل البيانات إلى صيغتها الأصلية وذلك باستخدام المفتاح المناسب لفك الشفرة[31].

والهدف من إجراء التشفير هو ضمان حفظ الخصوصيات وعدم السماح لأحد بالعبث بها أو الاطلاع عليها وذلك لكونها سرية أو خاصة جدا[32].

2- أهمية التشفير :

تكمن أهمية التشفير في التغلب على كثير من المخاطر و أذكر منها:

تجنب الإطلاع على المعطيات السرية والعبث بها، أو تغيير محتويات الرسائل المتبادلة، وتمنع محاولة تعديل البيانات المنقولة بالشبكة، أو إعادة توجيه البيانات إلى وجهة أخرى وكذلك اللجوء إلى تغيير كلمات السر الخاصة بالمستفيدين، أو انتحال شخصية المستخدم الحقيقي...الخ.

2.3. ضوابط التشفير

يقوم التشفير وفقا الضوابط والقواعد المتمثلة في:

1- إباحة تشفير البيانات والمعطيات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية.

2- احترام سرية البيانات المشفرة واعتراف بحق أصحابها في الخصوصية بتجريم الاعتداء عليها.

3- استخدام التشفير كوسيلة معتد بها قانونا في شأن تعزيز البيانات والمعطيات بواسطة الجهات المختصة.

3.3. مفاتيح فك التشفير

التشفير باستخدام المفتاح المتماثل واللامتماثل:

1- التشفير باستخدام المفتاح المتماثل:

يقوم هذا النظام على استخدام مفتاح متماثل للتشفير وحله، حيث يقوم المنشئ بعد كتابة الرسالة وتشفيرها بتزويد المرسل إليه بذات المفتاح المتماثل، ليتسنى له بعد تلقي الرسالة المشفرة حلها، واستعادة محتوى الرسالة في صورتها الأصلية.

2- نظام التشفير اللامتماثل:

هذا النوع من التشفير يستخدم فيه نوعين من المفاتيح، مفتاح عام وآخر خاص، أين يكون المفتاح العام متاح لكل شخص ويقتصر استخدامه على التشفير فقط، أما المفتاح الخاص فيكون شخصيا غير معروف إلاّ بالنسبة للمرسل إليه، ويقتصر استخدامه على حل شفرة الرسائل المشفرة بالمفتاح العام، إذ يقوم البنك أو المؤسسة بتزويد الزبائن بالمفاتح العامة وتستخدم هذه الأخيرة في تشفير الرسائل المتجهة إلى المؤسسة ولا يمكن استخدام المفتاح العام لفك شفرة الرسالة التي شفرها، وينفرد المفتاح الخاص لدى المؤسسة بالقدرة على فك شفرة الرسالة التي شفرها المفتاح العام[33]، وعليه يتم تشفير المعلومات طبقا لهذا النظام بالرقم العام، لكن لا يمكن فك الشفرة إلا بالمفتاح الخاص لصاحب المفتاح العام[34].

خاتمة

عمل المشرع على حماية الفرد من مخاطر الدفع الإلكتروني كتكريسه لقانون حماية البيانات الشخصية ، و القانون المتعلق بالتوقيع و التصديق الالكترونيين و القانون المتعلق بالتجارة الالكترونية و القانون المحدد لقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ... إن إنشاء مثل هذا القوانين يعتبر خطوة تقدم نحو الأفضل في تاريخ التشريع الجزائري لحماية البيانات الشخصية من الانتهاكات التي تحصل بحق خصوصية الأفراد، إلا أن هذا لا ينفي وجود بعض القصور في حماية المعطيات الخاصة من الانتهاكات التي تحصل عبر الوسائل الإلكترونية بالرغم من الجهود التي تبذلها الدولة في هذا المجال.

التوصيات

- يتعين على المشرع وضع نصوص تنظيمية لتبيان كيفية تطبيق أحكام القانون رقم 04/18 المحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، وكذا القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

- إحداث التوسع في ضمانات وأليات أكثر صرامة والمتعلقة بالأمن السيبراني من أجل حماية البيانات والمعطيات ذات الطابع الشخصي، لاسيما في شبكة التواصل الاجتماعي.

- أتضح جلّيا أن التدابير الوقائية المتوفرة حاليا غير كافية لأمن وسرية المعاملات الإلكترونية لمواجهة العبث الصادر من الغير بالأجهزة الإلكترونية، والذي يصعب أحيانا التعرّف عليه، عند قيامه بالتخريب وإتلاف والتجسس والتحايل ...الخ، لذا الواقع يلح على مواصلة البحث لإيجاد التدابير الوقائية أكثر صرامة لتصدي للأفعال الإجرامية التي ترتكب عبر شبكة الاتصال الإلكتروني.

الهوامش

1- فريد مشري، أمنة فاحة، لمزاودة رياض، الحماية القانونية لوسائل الدفع الإلكتروني، الجزائر نموذجا، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي، ضرورة الانتقال وتحديات الحماية 23 و24 أفريل 2018، المركز الجامعي عبد الحفيظ بو الصوف، ميلة، ص 03.

2- رجب عبد الحميد حسنين، أمن شبكات المعلومات الإلكترونية، المخاطر والحلول، جامعة الحصن، أبو ظبي، الإمارات العربية المتحدة، بدون سنة النشر، ص 04.

3- أ/ هداية بوعزة، د/ يوسف فتيحة، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مجلة الدراسات والبحوث القانونية، المجلد 03، العدد 04/ 2018، ص 2.

4- حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقايد، تلمسان، 2015، ص 354.

5-د/ كريمة شايب باشا، آليات الحماية من مخاطر الدفع الإلكتروني في التشريع الجزائري، المجلة الجزائرية لسياسات العامة، المجلد 07، العدد 02/ 2019، ص 40.

6- حوالف عبد الصمد، المرجع السابق، ص 355.

7- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، 2007، ص 15.

8- قانون رقم 18-07 مؤرخ في 25 رمضانه عام 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، المؤرخة في 10 يونيو 2018.

9- د/ محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، العدد الثالث والثلاثون، الجزء الرابع، كلية الحقوق، جامعة بنها، مصر، ص 1943.

10- ملياني عبد الوهاب، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه جامعة أبو بكر بلقايد، تلمسان، 2017، ص 40.

11- د/ منى تركي الموسوي، جان سيريان فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية 2013، ص 05.

12- المادة 42 من القانون رقم 18-07 السالف الذكر.

13- الفقرة الثالثة من المادة 07 من القانون رقم 18-07.

14- المادة 12 من القانون رقم 18-07.

15- المادة 13 من نفس القانون.

16- المادة 31 من نفس القانون.

17- المادة 10 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 مايو 2018 المحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ج ر عدد 27 المؤرخة في 13 مايو 2018.

18- طارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية، عبر الوسائل الإلكترونية في التشريع الأردني، مذكرة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط 2017، ص 58.

19- المادتين 07 و9 من القانون رقم 18-07 السالف الذكر.

20- فطيمة الزهراء مصدق، التصديق الإلكتروني كوسيلة لحماية التوقيع الإلكتروني، مجلة الدراسات والبحوث القانونية، المجلد 05، العدد الأول، 2020، ص 31.

21- قرواش رضوان، هيئات التصديق في ظل القانون رقم 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين (المفهوم والالتزامات)، مجلة العلوم الاجتماعية، العدد 24، 2017، ص 412.

22- مرسوم تنفيذي رقم 07-162 مؤرخ في 13 جمادى الأولى عام 1428 الموافق لـ 30 مايو سنة 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 15 صفر عام 1422 الموافق لـ 09 مايو سنة 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37 المؤرخة في 07 يونيو سنة 2007.

23- درار نسيمة، التوثيق الرقمي ومسؤوليته، سلطات المصادقة الإلكترونية في القانون الجزائري 15-04، مجلة الأستاذ الباحث للدراسات القانونية والسياسية 2019، العدد التاسع، المجلد الثاني، ص 857.

24- أ/ باهة فاطمة، شهادة التصديق الإلكتروني كآلية لضمان حجية المعاملات الإلكترونية في ضوء القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، مجلة البحوث في الحقوق والعلوم السياسية، العدد 20، دون سنة النشر، ص 389.

25- المادة 28 من قانون رقم 18-05 مؤرخ في 24 شعبان 1439 الموافق 10 مايو 2018 والمتعلق بالتجارة الالكترونية، ج ر العدد 28 المؤرخة في 16 مايو 2018.

26- درار نسيمة، المرجع السابق، ص 860.

27- الفقرات 01، 02، 03 من المادة 53 من القانون رقم 15-04. مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد06 المؤرخة 10 فبراير 2015.

28- حوالف عبد الصمد، المرجع السابق، ص 439.

29- رجب عبد الحميد حسنين، المرجع السابق، ص 05.

30- زهير زواش، دور نظام الدفع الإلكتروني في تحقيق المعاملات المصرفية – دراسة حالة الجزائر- مذكرة ماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة العربي بن المهيدي، أم البواقي 2011، ص 85.

31- صراع كريمة، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة ماجستير في العلوم التجارية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران 2014، ص 79.

32- زهير زواش، المرجع السابق، ص 62.

33- واقد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة ماجستير في القانون، كلية الحقوق جامعة تيزي وزو، 2011، ص164.

34- هداية بوعزة، يوسفي فتيحة، المرجع السابق، ص 33.